REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 04-05-2011	**2. REPORT TYPE** JMO Research Paper	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE "Network-Enabled" and "Leader-Centric" Command and Control (C2): The dangers of digital decision making	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Ryan R. McCaskill, Maj, USMC Paper Advisor (if Any): LTC Mark Bieger, LTC, USA	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
For Example: Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The DOD has grown increasingly reliant on information technologies (IT) that enable network-enabled command and control (NEC2). Evolving network-centric strategy documents focus too narrowly on improving the technological capabilities of existing C2 networks. The same documents fail to address the leadership challenges facing operational commanders who rely heavily on NEC2 systems. Connectivity, compatibility, and accessibility are three network vulnerabilities that limit the effectiveness of future NEC2 development. As the DOD applies technical solutions to technical problems, the joint services fail to address the unique NEC2 leadership challenges that could render future commanders less effective. Improved NEC2 capabilities could tempt commanders to rely too heavily on network information. Additionally, NEC2 provides commanders with the ability to assess and exert control over events at the tactical level. Modern operational commanders must pursue aggressive doctrinal and procedural modifications to reverse the cultural infatuation with achieving information dominance.

15. SUBJECT TERMS
Network-Centric Warfare, Command and Control (C2), Operational Command, Unity of Command, Network-Enabled

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		22	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

“Network-Enabled” Command and Control (C2): The dangers of digital decision making

by

Ryan R. McCaskill

Major, USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ________//signed//_________

4 May 2011

Contents

Abstract

The Department of Defense (DOD) has grown increasingly reliant on the information technologies (IT) that enable network-enabled command and control (NEC2). Evolving network-centric strategy documents focus too narrowly on improving the technological capabilities of existing C2 networks. The same documents fail to address the leadership challenges facing operational commanders who rely heavily on NEC2 systems. Connectivity, compatibility, and accessibility are three network vulnerabilities that limit the effectiveness of future NEC2 development. As the DOD applies technical solutions to technical problems, the joint services fail to address the unique NEC2 leadership challenges that could render future commanders less effective. Improved NEC2 capabilities could tempt commanders to rely too heavily on network information. Additionally, NEC2 provides commanders with the ability to assess and exert control over events at the tactical level. Modern operational commanders must pursue aggressive doctrinal and procedural modifications to reverse the cultural infatuation with achieving information dominance.

> *DOD C2 must be leader-centric and net-enabled to facilitate initiative and decision-making at the lowest level possible…[T]he phrase "leader-centric and net-enabled" refers to a balance between the art of war (human interface) and the science of war (technological solutions)…[T]he principal maxim of command and control: technology enables human interface and supports "command" and the decision maker, rather than forcing the decision maker to operate within the constraints of "control" technology…*
>
> *Department of Defense C2 Implementation Plan v 1.0(2009)*[1]

Network-enabled and Leader-Centric Command and Control (C2)

Network-enabled command and control (NEC2)[2] systems present an operational commander with two distinct leadership challenges. First, NEC2 systems tempt commanders to rely too heavily on the network technologies that contribute to a commander's situational awareness (SA). Second, NEC2 systems provide commanders with the technological capability to focus too narrowly on the tactical level of war. This capability tempts operational commanders to ignore the most fundamental maxim of the American C2 process: centralized command and decentralized execution. Collectively, NEC2 technologies negatively influence the C2 process at the operational level. To counteract the negative influence, operational commanders must encourage the modification of existing technology-centric doctrine and implement procedures that leverage alternative C2 processes and inspire a more leader-centric command force.

To support the claim that network-enabled technology detracts from the C2 process, this essay attempts to answer the following questions. What is NEC2? How do networked systems contribute to a commander's understanding of the battle space? Is there any evidence that suggests operational commanders have become too reliant on network-enabled technologies? Do NEC2 systems tempt commanders to focus too narrowly on the tactical fight? And finally, how might future operational commanders avoid becoming overly reliant

[1] p. 15

[2] NEC2 is an acronym that is unique to this essay. Joint doctrine has yet to coin an acronym for network-enabled command and control.

on network-centric systems? This essay examines these questions in four sections. The first section defines NEC2 and describes how network systems influence the commander's decision process. The second section examines the perils that may befall a commander who relies too heavily on network-enabled information systems. The third section examines network capabilities and the resultant tactical temptations that prompt operational commanders to overextend their C2 influence at the tactical level. Finally, this essay attempts to reconcile the rapidly evolving technological capabilities against a C2 process that demands a greater degree of human interface.

What is NEC2? Grappling with an evolving conceptual definition

The current *Department of Defense (DOD) C2 Implementation Plan (v1.0)* envisions a C2 process that is "leader-centric and net-enabled."[3] Ideally, this process leverages emerging network technologies to enhance a commander's ability to make faster and more well-informed decisions. Unfortunately, the evolving nature of the NEC2 concept makes it difficult to grasp the true meaning of "network-enabled" C2 process. Establishing a common definition of NEC2 is difficult because one must narrowly account for the vague amalgamation of cyberspace infrastructure that enables the collection, collation, and distribution of information over integrated communication networks. Though difficult, establishing a baseline definition of NEC2 is important because one must understand *what* NEC2 actually *is* before one understands *how* network-enabled technology negatively influences the decisions of the modern operational commander. A proper understanding of NEC2, therefore, requires one to account for the tangible and intangible components that enable network connectivity and information distribution.

[3] DOD C2 Implementation Plan, p. 5

According to the C2 Implementation Plan, “net-enabled” is a term that accounts for a*ll* of the interconnected information technology systems that facilitate C2 operations.[4] This definition includes the tangible hardware systems—people, sensors, and platforms—that contribute data to the network, as well as the software systems and servers that filter, fuse, and process varied data inputs. Collectively, the hardware and software systems interact to generate a common operating picture (COP).[5] According to this technical definition, NEC2 is a term that refers to a series of networked systems that incorporate data in order to produce an objective operational picture. The commander, in turn, references the COP in order to enhance his awareness of the operational surroundings. In theory, the COP provides a commander with the ability to make more accurate and well-informed decisions. Unfortunately, any NEC2 definition that limits itself strictly to the tangible characteristics of the network fails to accurately account for *how* intangible network components such as speed of information flow or quantity could influence the C2 process. Put differently, existing doctrinal definitions imply that access to high-quality information automatically results in high-quality decisions. To properly understand the *entire NEC2 process* however, one must also account for *how* network technologies manipulate information, enable human interface, and influence the decision makers in command.[6] In this light, one must define NEC2 as a two phase process where a “leader-centric” *process* relies on a “network-enabled” *product*. Network-enabled technology produces an informational output in the form of a COP. Commanders leverage the network *product* to inform the *leader-centric* decision *process*. Successfully balancing the demands of a growing “network-enabled” COP against the rigors

[4] DOD C2 Implementation Plan, p. 6

[5] The most prominent example of an operational NEC2 system that produces a COP is The Global Command and Control System (GCCS). While the technical capabilities of GCCS go beyond the scope of this essay, the reader should reference http://www.disa.mil/gccs-j/index.html for a detailed explanation of how GCCS contributes to the NEC2 COP.

[6] DOD C2 Implementation Plan, p. 7

of intelligent “leader-centric” decisions is the key to understanding the NEC2 concept, and subsequently understanding why it is dangerous.

Ideally, network-enabled technology allows commanders to develop rapid and accurate assessments of battlefield conditions. However, the NEC2 concept rests on the implicit notion that a commander who *sees* the battlefield though the lens of a digital COP also *understands* the battlefield. Indeed, the cognitive link between information access, and understanding or awareness, is the subject of much debate.[7] NEC2 proponents believe that technological capabilities provide commanders with information that can “influence decision-making and enhance effective execution.”[8] Opponents, meanwhile, argue that NEC2 technology provides commanders with shared information, but do not *necessarily* generate a sense of shared awareness.[9] In *Dynamic Theory of Organizational Knowledge Creation*, Nonaka argues that “although the terms ‘information’ and ‘knowledge’ are often used interchangeably, there is a clear distinction between information and knowledge.”[10] While the cognitive link between awareness and understanding is beyond the scope of this essay, the effectiveness of NEC2 quite obviously depends on the accuracy and timeliness of the information that informs command decisions. The core issue in framing the NEC2 dilemma therefore, is *not* whether networked systems provide more or less information to the commander.[11] Instead, the true nature of the NEC2 debate is *how* more or less information influences the C2 decision process. Does a commander always benefit from having access to *more* information? Conversely, what happens if the network is compromised and the flow of

[7] Refer to Sofge and Bates for a more detailed account of the academic debate about differences between information access and awareness/understanding. See bibliography.
[8] Sofge, p. 4
[9] Elward, p. 10
[10] Sofge, p. 10
[11] This essay does not dispute the fact that NEC2 systems undoubtedly provide commanders with much greater access to information than ever before. The issue at hand is whether more information is good for the commander.

information stops or becomes corrupted? Would the subsequent lack of network-enabled information help or hinder the C2 process?

Although network-enabled technology gives commanders greater access to information, the sheer quantity of data does not always create a more efficient C2 process. NEC2 depends on information collaboration efforts within an operational chain of command. Collaborative efforts allow subordinate units to provide network updates to the commander who uses the fused COP to keep abreast of real-time developments. To enable widespread collaboration, the *DOD C2 Implementation Plan* envisions a NEC2 structure that provides "pervasive and persistent access to multi-level, multi-source data and mission-tailorable services when and where needed by authorized users."[12] "Pervasive and persistent access" implies that subordinate units have the ability to contribute to the COP as well as act on information provided by the COP—anywhere and anytime. However, developing a system architecture that allows for broad and consistent network participation creates a quandary for operational commanders. To illustrate the point, consider how the fidelity of the COP is subject to change based on the quantity, accuracy, or frequency of subordinate unit contributions. For this reason, a commander derives greater benefits from a COP that incorporates *more* unit data on a *more* frequent basis. *Fewer* multi-source contributions on the other hand, limit the scope and accuracy of the operational picture. Thus, in order to maximize the efficiencies offered by the NEC2 process a commander should endeavor to provide some level of network access to as many subordinate units as possible. A problem arises however, when unit contributions become contradictory or grow so cumbersome that they overwhelm the COP integration process.[13]

[12] DOD C2 Implementation Plan, p. 29

[13] This integration process is often referred to as information "fusion". Fusion is the process of combining multiple data inputs into a single informational output. This "processed information" is what a commander studies to gain greater awareness of the battlefield.

When the network contributions exceed the abilities of the end-user, commanders and their staffs may suffer from information overload. Information overload is, simply, an "excess of information that results in the loss of ability to make decisions, process information, and prioritize tasks."[14] To avoid overtaxing the networks or the people using the net-enabled information, commanders must create C2 networks that are accessible, but not *too* accessible. In addition, commanders must understand how net-enabled collaboration tools have reshaped the C2 system.[15] Specifically, net-enabled collaboration has altered the structure of the traditional operational chain of command. Traditionally, the C2 process has relied on the concept of vertical information sharing. Information was "stove-piped" through service-specific networks to intelligence analysts and up the chain of command[16]. While the commander had access to the entire operational picture, subordinate units maintained limited access to smaller pieces of the puzzle. Modern NEC2 enables—in fact, *requires*—greater collaboration between subordinate units. As a result more people within the operational chain of command have access to the COP and develop different interpretations of the digital picture. This collaboration has effectively changed the C2 structure from a vertical hierarchy to a horizontal partnership. Network-enabled technology allows commanders and subordinate units an opportunity to interact within the network and contrast or compare their understanding of the battlefield. This collaboration discourages the historical means of passing information *up* the chain of command, and encourages units to pass information *laterally within* the chain of command. This sharing relationship carries a significant consequence for the operational C2 system. Specifically, as more units reap the benefits of

[14] Martin, p. 6

[15] Net-enabled collaboration tools are also referred to as service oriented architectures (SOA) or "cloud" based services, or mash-ups. In each case, these "tools" accept multiple data inputs from varied platforms and systems and fuse the data into a single informational output.

[16] "Stovepiped" is a term that refers to vertical structure of service specific networks that have, in the past, precluded the lateral sharing of information. Lack of technological standardization amongst services has often created system incompatibilities that forced units to stovepipe information to the commander rather than share it with adjacent units.

greater information access, the operational units will tend to immunize themselves against the impossible notion of an information deficit. In short, commanders are tempted to ignore the difficulties that a lack of net-enabled information access would surely create.

One of the greatest temptations facing commanders is the belief that network-enabled capabilities will eliminate uncertainty on the battlefield. In the pursuit of absolute certainty, and ignoring the historical significance of fog and friction, the C2 process may slow or stop as commanders wait for more detailed information to filter through the network.   Such a delay could force an operational commander to alter the operational tempo as the decision process becomes subservient to lag in information processing. Though counterintuitive, growing evidence supports the claim that more information slows the C2 decision process. A study by Dr. Douglas Peters concludes that "commanders and their staffs are addicted to information."[17] This addiction causes commanders "to delay important decisions in order to pursue an actual or perceived possibility of acquiring additional information."[18] While more information delays the decision process, it also has the potential to detract from a commander's understanding of the operational picture. To illustrate the point, Dr. Peters suggests that access to more information drives commanders to apply a "more shallow cognitive process to the overall picture."[19] In light of this study, it appears that commanders may take longer to understand and act upon the information produced by the NEC2 technologies. To prevent NEC2 technologies from paralyzing the C2 process, commanders must understand how they use—and rely on—network-enabled information systems. In short, operational commanders must avoid becoming too reliant on the network systems that enable C2 functionality.

[17] Bates, p. 8
[18] Ibid.
[19] Ibid. p. 14

Network Reliance: Balancing NEC2 utility against technological dependency

An overreliance on NEC2 technologies poses two risks for operational C2. First, peacetime connectivity tempts commanders to *ignore* the technical vulnerabilities inherent in network operations. The second risk is a byproduct of the first: ignoring network vulnerabilities gives commanders a false sense of information dominance and prompts NEC2 users to inflate the capabilities that NEC2 offers in a peacetime training environment. Collectively, the temptation to *ignore* NEC2 vulnerabilities and *inflate* the technological capabilities sets a dangerous precedent for future decision makers.

In theory, NEC2 gives an operational commander access to greater volumes of accurate and timely battlefield information. NEC2 proponents believe that access to more information allows commanders to make faster and more well-informed decisions. In essence, proponents believe that NEC2 has the potential to reduce or eliminate the fog of war.[20] Though enticing, such arguments fail to consider how thick the fog might become if the network falls victim to a disruptive attack. For this reason, commanders who rely heavily on network-enabled technologies must continually remind themselves of two critical vulnerabilities in the NEC2 concept. First, a commander must accept the fact that a network-enabled COP may never uncover or recognize the "ground truth."[21] Second, network technology cannot "identify or articulate uncertainty through its medium."[22] Existing doctrine inculcates commanders with the notion that NEC2 technology is always timely and accurate.[23] As such, it is difficult for commanders to counteract the temptation of waiting longer for the "ground truth" to reveal itself, or moving forward with a decision under a false sense of certainty. As a result, commanders rely on NEC2 technology to "eliminate doubt or

[20] Elward, p.
[21] Kemmerer, p. 12
[22] Ibid.
[23] Kemmerer, p. 12.

uncertainty" rather than viewing the COP as a suspect companion that might, at any moment, revolt against its owner.[24] While existing doctrine reinforces the belief that DOD systems can exchange secure and reliable information "in both optimum and degraded information-sharing environments," commanders lose the incentive to develop or practice alternative methods of command and control.[25] The lack of alternative C2 processes could prevent US forces from countering a hostile attack that attempts to exploit the vulnerabilities common to all networked communication systems.

NEC2 systems are only useful when the information they present is secure and reliable. Unfortunately, the NEC2 infrastructure is vulnerable to three types of disruption that could limit the availability or authenticity of the COP, and thereby degrade the C2 decision process. First, units within the operational chain of command retain different levels of network connectivity. Second, system incompatibilities within operational commands limit the utility and distribution of fused information outputs. Finally, different network access permissions alter the accuracy and the utility of the COP.[26] Each of the three vulnerabilities poses different challenges for the operational commanders and subordinate units who rely on the system. Limited connectivity, for example, may prevent a commander from communicating with subordinate units while system incompatibilities may prevent critical information from being fused into a COP. In each case, a cyber-attack that targets any of these vulnerabilities could limit or corrupt network information. This exploitation would make it more difficult for a commander to decipher the COP and communicate with subordinate units. Additionally, such an attack would require commanders to fall back on alternative forms of C2, or depend on leaders capable of making C2 decisions without the aid

[24] Kemmerer, p. 12.
[25] DID C2 Implementation Plan, p. 29.
[26] The recent wiki-leaks incident is a perfect example of how broad access permissions pose additional security risks for operational commanders.

of NEC2 information. Commanders who are over reliant on NEC2 technologies may marginalize the technical weaknesses of NEC2 systems. On the other end of the spectrum, the capabilities and strengths of NEC2 systems may tempt commanders to place a premium on the technological capabilities that enable direct control at the tactical level.

<u>Network-Enabled or Network-Excessive: "Over-commanding" and "over-controlling"</u>

Recognizing, or overcoming, an excessive reliance on NEC2 systems creates an even greater predicament for operational commanders. Mainly, NEC2 technology provides commanders with the ability—and subsequent temptation—to use network systems to exert direct control at the tactical level. In simple terms, NEC2 capabilities tempt commanders to move away from the traditional concept of centralized command and *decentralized* execution. Instead, NEC2 systems force commanders to create organizational cultures that place a premium on *centralized* control and *centralized* execution. In military parlance, "centralized control" is more commonly referred to as "micromanagement." To be clear, this section does not contend that NEC2 systems will *necessarily* produce a new generation of commanders who use technology to micromanage their operational forces. Nor does this section intend to generalize or project negative leadership characteristics or personal experiences onto current or future operational commanders. Instead this section explores the growing body of evidence that suggests a direct correlation between NEC2 systems and the continued development of command climates that tolerate network-enabled micromanagement. While exploring this evidence, one must bear in mind that NEC2 capabilities will not automatically generate command climates that accept or value centralized execution. Certainly a commander's personal leadership style inevitably influences how an organization uses or depends on technology. In the long term however, improper use of NEC2 could dissuade the cognitive development of subordinate leaders who act decisively without waiting for higher command approval. Commanders must understand both the technological temptations and negative C2 consequences before designing and implementing measures that limit the widespread misuse of NEC2 authority.

Several academic studies examine the phenomena of network-*excessive* C2 (micromanagement). Each study attempts to explain *why* NEC2 tempts commanders to exert control at the tactical level, and examine *how* their actions impact the C2 process. As early as 2001, the U.S. Navy conducted a study to examine the effectiveness of decentralized joint fires. After action reports from the Fleet Battle Experiment-India exercise concluded that "given the visibility of modern tactical operations to upper command echelons and the media," commanders had additional incentives to micromanage action at the tactical level.[27] In this face of such pressures, operational commanders had "considerable difficulty allowing decentralized execution."[28] While the Fleet Battle study examines the underlying cultural motivations, a documented incident with General Wesley Clark provides the best example of how improper network use can affect the C2 process. Although far removed from the battlefield, General Clark thought he recognized three tanks on a digital screen in a joint C2 center. NEC2 technology allowed him to "pick up a telephone, call the joint forces air component commander, and direct that those tanks be destroyed. [W]ith a single call, based on incomplete information, all the levels of war, from strategic to tactical, had been short-circuited."[29] Given that the objects were not actually hostile tanks, General Clark's actions provide two important lessons. First, commanders should not assume that a digital COP provides a level of fidelity that enables intelligent, or necessary, command decisions. Second, NEC2 capabilities have the potential to obscure command relationships. To

[27] Vassilliou, p. 13.
[28] Ibid.
[29] Ferris, p. 8

illustrate the point, consider an operational commander who frequently uses NEC2 to influence action at the tactical level. Such action may create subordinate leaders who are hesitant to exercise direct control over their assigned forces for fear or expectation of higher C2 intervention. To prevent commanders from falling victim to the tactical temptations created by NEC2, the joint community must modify existing doctrine so that it speaks clearly to the dangers of centralized command and centralized execution.

The Way Ahead: Untangling ourselves from technological temptation

Operational commanders must take two steps to mitigate the risks and temptations that accompany net-enabled operations. First, operational commanders must address the *doctrinal* failings that permeate current NEC2 documents. Second, commanders must implement *procedural* changes that alter the way units prepare for, and conduct, major operational exercises. Essentially, the second step entails a thorough examination of the existing tactics, techniques, and procedures (TTPs) that would allow commanders to assert effective C2 following the loss of the net-enabled architecture. Ideally, the doctrinal changes would precede and subsequently inspire procedural changes.[30] As such, this section examines the current doctrinal failings before outlining a sampling of recommended procedural changes. In each case, the doctrinal and procedural modifications should dissuade commanders from becoming overly-reliant on the NEC2 system, or using the technology to focus too narrowly on the tactical level or war.

Current NEC2 doctrine suffers from two major weaknesses. The first glaring doctrinal weakness is an unrealistic infatuation with future technological capabilities. The DOD Information Enterprise Architecture (IEA) Strategic Plan for 2010-2012 claims that the

[30] How doctrine influences (or contributes to) the "officially sanctioned approach to military actions" is a tenuous link. Paul Johnston argues that "doctrine may be more an effect than a cause." This would imply that the current cultural emphasis on technology has an inertia of its own and doctrinal modifications may or may not be able to reverse the momentum of technological reliance. Johnston, p. 6

DOD is “moving rapidly toward achieving a service-oriented information enterprise.”[31] In this enterprise, “all data assets, services and information-sharing solutions” will be “visible, accessible, understandable, and trusted by all authorized users, except where limited by law, policy or security classifications.”[32] Providing broad information access should allow the DOD to obtain an “information advantage” that serves as “a source of power and a force multiplier” for U.S. forces.[33] Admittedly, the IEA Plan is a strategy document—not joint doctrine. Nonetheless, the IEA Strategic Plan *is* in line with the conceptual C2 capabilities put forth in Joint Pub 3-0 (JP-3-0). JP-3-0 envisions a NEC2 process that allows commanders to leverage “judgment and intuition acquired from experience” to complement the technologies that enable “information management and awareness of the operating environment.”[34] Collectively, the sound leadership “experience” and network-enabled “awareness” should “facilitate” a decision process that “provides commanders with the ability to make timely decisions and execute those decisions more rapidly than the adversary.”[35] Most importantly, this decision enhancing capability will “decrease risk and allow the commander more control of the timing and tempo of operations.”[36] At first glance, it seems existing joint doctrine recognizes the importance of the human component in the C2 process. A more detailed examination, however, reveals a doctrine which is heavily weighted in favor of greater technological integration and less leader-centric C2 input.

Although modern C2 doctrine stresses the importance of the human actor, there is a noticeable imbalance between the future technological expectations, and the emphasis placed on the future development of commander’s cognitive capabilities. Put differently, modern

[31] DOD IEA Strategic Plan 2010-2012, p. 1
[32] Ibid.
[33] Ibid.
[34] JP-3-0, p. III-2
[35] Ibid., p. III-3
[36] DOD IEA Strategic Plan 2010-2012, p. 3

doctrine devotes too much attention to describing how technological expansion will further expand NEC2 capabilities. At the same time, doctrine devotes too little attention to the future cognitive development of leaders who will use—*or be used by*—the system. The current DOD C2 Implementation plan states that "leader-centric" NEC2 process is "a balance between the art of war (human interface) and the science of war (technological solutions)"[37] [T]he principal maxim of command and control: technology enables human interface and supports "command" and the decision maker, rather than forcing the decision maker to operate within the constraints of "control technology."[38] Unfortunately, balancing the human and technological solutions is a goal that falls by the wayside within the larger context of a document that focuses on how to develop agile and robust capabilities that can "meet the operational demands of a persistent conflict environment."[39] Moreover, even though C2 technologies are sure to change and the idyllic NEC2 capabilities may—or may not—be realized, the human capacity to accept and process more information is not likely to keep pace. For this reason, future doctrine should emphasize the development of critical decision-making skills, rather than the benefits offered by the development of more robust technological networks. Indeed, these skills will be required in the event that a capable opponent finds a way to disrupt or disable the architecture that supports the NEC2 system.

Another doctrinal flaw common to modern NEC2 documents is the underlying presumption that networks are simultaneously infallible and invincible. Existing NEC2 strategy documents presume that network redundancies will provide security and resiliency in the face of sustained or complex network attacks. As a result, operational doctrine reflects the belief that commanders will retain at least *some* capacity to "work through" network

[37] DOD C2 Implementation Plan, p. 15
[38] Ibid., p. 6
[39] Ibid., p. 29

attacks that add friction to the network-enabled process.[40] Additionally, the DOD IEA Strategic Plan puts forth the notion that a further expansion of NEC2 capabilities will "provide accurate and timely information about network health and mission readiness to decision makers at all levels, along with the control capabilities they need to implement C2 decisions for mission success."[41] This capability should, doctrine holds, allow commanders to understand whether friendly C2 networks are compromised so that they might switch to more secure network systems. Theoretically then, future networks will not only eliminate uncertainty on the battlefield, but also recognize enemy efforts to introduce uncertainties into the networks. While these capabilities would certainly create a distinct advantage, the likelihood of an NEC2 process which is simultaneously all-knowing and self-aware is not realistic. Further, the development of doctrine that focuses on *potential technological capabilities* rather than the *historical certainty* that war is by nature *uncertain,* carries second order consequences. The byproduct of technologically focused doctrine is that operational commanders have had little incentive to develop alternative C2 processes or procedures that would fill the void if NEC2 systems are compromised.

To account for unforeseen network limitations, commanders should develop alternative C2 processes that depend more heavily on traditional forms of communication. These alternative processes would allow commanders to practice decision making without the aid of a digital COP and exercise communication methods that modern commanders may consider technologically obsolete. Put simply, modern operational commanders need to develop C2 capabilities that presume a complete *lack* of a network-enabled system, rather than a *partially capable* network system. Developing these skills requires regular large-scale

[40] DOD IEA Strategic Plan 2010-2012, p. 20
[41] Ibid., p. 14

training exercises where commanders exercise C2 without the aid of satellite communications, email, or chat. Additionally, commanders should eliminate the use of the COP or intentionally introduce false information into the problem to evaluate whether subordinate units are capable of efficient and intelligent decision-making in the face of limited or non-existent information. Pilots need to conduct regular training without the aid of digital networks (e.g., Link-16) that enhance their SA or network dependent precision guided weapons. Ground force commanders need to conduct movement and maneuver exercises without the aid of a Blue Force Tracker. These maneuvers should gradually escalate into live-fire combined arms exercises where radio communication and intelligent prepositioning of forces is the only means of effective C2. The above ideas are just a sampling of procedural changes which commanders must regularly demand from their subordinate units. After all, a failure to maintain alternative C2 processes at the operational level in peacetime may have catastrophic consequences at all three levels of war in a fast-paced large-scale conflict.

Conclusion

This essay does not intend to suggest that NEC2 is a flawed concept. In truth, NEC2 presents the U.S. military with an opportunity to capitalize on comparative cyber advantages that could prove to be *the* decisive capability in a future conflict. That said, operational commanders must balance the benefits offered by NEC2 *capabilities* against the technological *risks* inherent to any network operations. To mitigate these risks, operational commanders must ensure that subordinate units are prepared to operate for prolonged periods without access to NEC2 systems. Such a prohibitive environment demands alternative C2 processes. To prepare for this eventuality, commanders should modify existing doctrine and procedures. In each case, the doctrine and TTPs should promote the development of alternative C2 processes. The alternative processes should be founded on the assumption that the NEC2 grid is neither sufficiently redundant nor immune to a disabling network attack. To adequately prepare for such an occurrence, commanders should mandate annual training requirements that stress independent decision making in a complex environment. These training evolutions will become increasingly more important as non-network prone commanders—e.g. the "old" school—vacates the higher echelons of command. In their place, the first generation of touch-screen, net-enabled commanders will take the helm. While subsequent generations of commanders are sure to possess a solid understanding of the network capabilities and limitations, they are likely to be less prepared for the complexities and challenges offered by a world where network connectivity becomes either suspect or impossible. Unfortunately, falling victim to these technological temptations will force commanders to relearn lessons from the past. Describing the action at Leyte Gulf, Herman Wouk writes, "[T]here never was a denser fog of war. All the sophisticated communication only spread and thickened it."[42] To cut through the increasingly thick layers of fog, operational commanders should take advantage of the capabilities that NEC2 *offers*, but they must prepare C2 alternatives that a lack of a network access would *require*. Focusing on the development of a leader-centric command force, rather than an expansion of technological dominance may ultimately prevent network-enabled failure in the next major conflict.

[42] Wouk, Herman, p. 930.

BIBLIOGRAPHY

Assistant Secretary of Defense (Networks and Information Integration)/DOD Chief Information Officer, "Vision/Mission." "Defense Link." n.d. http://www.defenselink.mil/cio-nii/docs/card.pdf (accessed March 17, 2011).

Barker, Robert A. *Command and Control of Network Operations.* Strategy Research Project, Carlisle Barracks, Carlisle Barracks, PA: U.S. Army War College, Mar, 2009.

Barlow, David A. *Impeding Network Centric Warfare: Combatant Command Information Technology.* Strategy Research Project, Carlisle Barracks, Carlisle Barracks, PA: U.S. Army War College, Feb, 2009.

Bates, Chad. *The Battle of Cognition against the Tyranny of Information Overload.* Masters Thesis, Joint Military Operations, Newport, RI: Naval War College, May, 2010.

Cartwright, James E. *Joint Concept of Operations for Global Information Grid NetOps version 3.* Memorandum, Offut Air Force Base, NE: USSTRATCOM, August 4, 2006.

Douglas J. Peter, et al. "The Time to Decide: How Awareness and Collaboration Affect the Command Decision Making." In *Battle of Cognition*, edited by Alexander Kott. Westport, CT: Praeger Security International, 2008.

Elward, Sean M. *The Fog of War: A Necessary Component of Modern Warfare.* Masters Thesis, Joint Military Operations, Newport, RI: Navy War College, May, 2010.

Ferris, John. "A New American Way of War? C4ISR in Operation Iraqi Freedom, A Provisional." *Journal of Military and Strategic Studies* 6, no. 1 (2003): 12.

Grimes, John G. *Department of Defense NetOps Strategic Vision.* Washington, D.C.: The Pentagon, September, 2008.

Hellström, Tomas. "ScienceDirect." *www.sciencedirect.com.* July 8, 2006. http://www.sciencedirect.com/science/article/B6VF9-4M3RP2W-1/2/6455be82934e3539b0ab207b80b22dec (accessed Feb 16, 2011).

Johnston, Paul. "Doctrine Is Not Enough: The Effect of Doctrine on the Behavior of Armies." *Parameters* 30, no. 3 (Autumn 2000): 30-39.

Kemmerer, Kacey Edward. *Tactical Decision Making Under Categorical Uncertainty With Applications to Modeling and Simulation.* Master's Thesis, Monterrey, CA: Naval Postgraduate School, Dec, 2008.

Korns, Stephen W. "Cyber Operations: The New Balance." *Joint Forces Quarterly* (National Defense University Press), no. 54 (3d quarter 2009): 97-102.

Martin, Darryl B. *Knowledge Management: An Effort to Keep Pace with Information.* Masters Thesis, Joint Military Operations, Newport, RI: Naval War College, May, 2009.

Michael W. Kessler. *Coping with Uncertainty: Command and Control in Information Degraded Environments.* Masters Thesis, Joint Military Operations, Newport: Naval War College, Jun, 2010.

Nonaka, Ikujiro. ""A Dynamic Theory of Organizational Knowledge Creation."." *Orginization Science* 5, no. 1 (1994): 19.

Phister, Paul W. and Igor G. Plonisch. *Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare.* Research Paper, Information Directorate, Rome, NY: Air Force Research Laboratory, Jun, 2004.

Regoli, Elizabeth A. *Network Centric Warfare's Impact on Future Leader Development.* Masters Thesis, Joint Military Operations, Newport, RI: Naval War College, Jun, 2009.

Smith, Barry, Kristo Miettinen, William Mandrick. *The Ontology of Command and Control (C2).* In Proceedings of the 14th International Command and Control Research and Technology Symposium, Buffalo, NY: National Center for Ontological Research, Jun, 2009.

Smith, Daniel K. *An Analysis of Defense Information and Information Technology Articles: a sixteen year perspective.* Masters Thesis, Wright Patterson AFB, OH: Air Force Institute of Technology, Mar, 2009.

Sofge, Robert. *Knowledge Centric Warfare: An Introduction.* Strategy Research Project, Carlisle Barracks, Carlisle Barracks, PA: Army War College, Mar, 2009.

U.S. Departement of Defense. *Command and Control Implementation Plan, VERSION 1.0.* Memorandum, Washington, D.C.: U.S. Department of Defense, Assistant Secretary of Defense (Networks and Information Integration), 1 OCT 2009.

U.S. Department of Defense. *Data Sharing in a Net-Centric Department of Defense.* Directive 8320.02, Washington, D.C.: Department of Defense, Assistant Secretary of Defense (Networks and Information Integration)/Department of Defense Chief Information Officer, 2 Dec 2004.

U.S. Department of Defense. *Department of Defense Information Enterprise Architecture (IEA) Version 1.2.* Directive, Washington, D.C.: Department of Defense, Office of the Chief Information Officer, May 7, 2010.

U.S. Department of Defense. *Doctrine for the Armed Forces of the United States.* Joint Publication 1, Washington, D.C.: U.S. Department of Defense, n.d.

U.S. Department of Defense. *Information Technology Portfolio Management.* Directive 8115.01, Washington, D.C.: U.S. Department of Defense, Assistant Secretary of Defense (Networks and Information Integration), October 10, 2005.

U.S. Department of Defense. *Management of DOD Information Resources and Information Technology*. Directive, 8000.01, Washington, D.C.: U.S. Department of Defense, Assistant Secretary of Defense (Networks and Information Integration), February 10, 2009.

U.S. Secretary of Defense. *Department of Defense Information Enterprise Strategic Plan 2010-2012.* Directive, Washington, D.C.: Office of the Assistant Secretary of Defense (Networks and Information/Integration) and DOD Chief Information Officer, April 1, 2010.

Vassiliou, M.S. *The Evolution Towards Decentralized C2.* Technical Report, Alexandria, VA: Institute for Defense Analyses, Jan, 2010.

Vego, Milan. "Systems versus Classical Approach to Warfare." *Joint Forces Quarterly* (National Defense University Press), no. 52 (1st Quarter 2009): 40-48.

Wouk, Herman. *War and Remembrance.* New York: Little Brown and Company, 1978.